Starting to Oauth 2.0

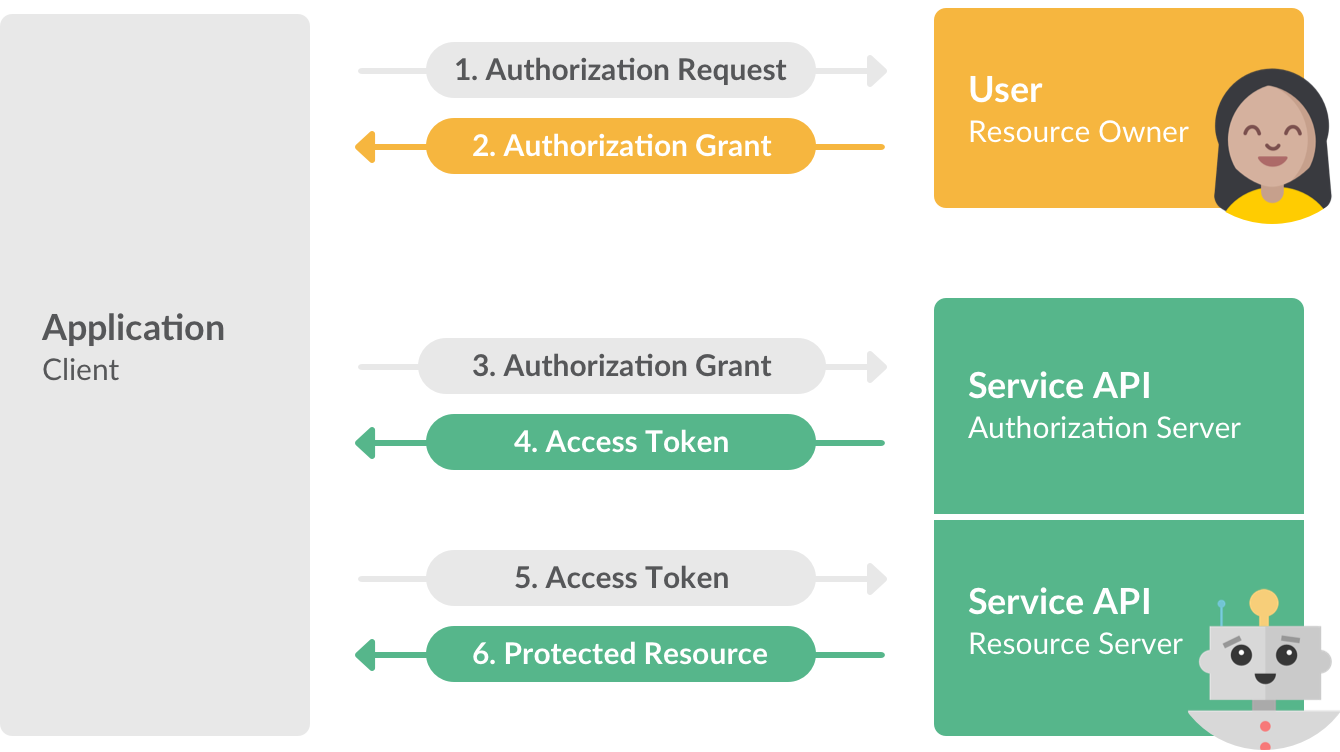
## Question 1: What is Oauth 2.0 ?

Oauth 2.0 is a open standard protocol for authentication and authourization to web app and apis. It’s actual definition can only be understood if you know its five basic pillers-

1. Resource- A resource can be understood as the details you provide, when you sign up or register on any website or application. For an instance, email-id and password of gmail account is a resource of you.
2. Resource Owner- One, who use create and use them is known as Resource Owner. For example, you are a resource owner, Whose resource can be gmail account details.
3. Resource Server- One, who take care of your resources can be defined as Resource server. For example, Google take care of your gmail account details, So It is a Resource Server.
4. Client Application- It is the web application that you want to access with your resources. For example, If you want to access linked-in website, you can use gmail account details for signup. So in this case, linked-in website is a client application.
5. Authorization Server- It provides you a token, by which you will able to access the Client Application. Most of the times, It is same as resource server.

Now, Back to Oauth definition-

This protocol allows Client Application to access your resource for authourizing you with Authorization Server. After that, When Authorization server verifies you, It issues a token. With help of this token, you can use Client application rather than any credential details.



## Question 2: What is Token?

Token is a random string that is generated by Authorization Server. There are two type of tokens-

1. Access token- When the Authorization server issues a token to client application on request of client application, Client application get limited access to your resource available at resource server.

It have some limited life, which is defined by authorization server itself..

1. Refresh token- It is also issued at same time when access token is issued. But due to short life of acccess token, access token expires. When the access token expires, client application use refresh token to generate a new access token.